PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-145475
(43)Date of publication of application : 20.05.2004

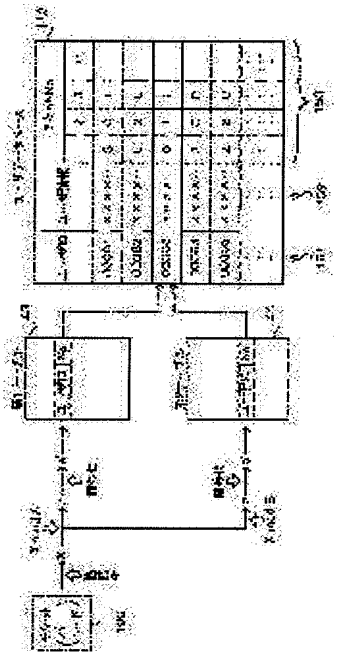
(51)Int.Cl. G06F 15/00
G06F 12/00
G06F 17/60
G06K 7/00
G06K 7/10
G06K 17/00
G06K 19/07
G09C 1/00
H04L 9/32

(21)Application number : 2002-307471
(22)Date of filing : 22.10.2002

(71)Applicant : PATENT ONE KK
(72)Inventor : UGAWA TARO
FURUMIZO SATOSHI

(54) IDENTIFICATION INFORMATION ISSUE SYSTEM AND METHOD, IDENTIFICATION INFORMATION AUTHENTICATION SYSTEM AND METHOD, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To accomplish both speed-up of an authentication process of identification information and improvement of security, and to allow each user to selectively use a plurality of pieces of identification information without increasing a processing amount.
SOLUTION: When an issue request including a user ID and a ticket No. is present, a ticket of a random pattern is generated and is digitalized. Residues (a), b are found by dividing the numerical value by divisors A, B, and an encrypted value a', b' are generated by encrypting the residues (a), b. When the same set is not registered in a storage position of the encrypted value a' of a first table 143 and a storage position of the encrypted value b' of a second table 144, the set of the user ID and the ticket No. included in the issue request is registered, and the ticket is transmitted to a request source. When the transmitted ticket is inputted, the encrypted values a', b' are similarly generated, and the ticket is authenticated when the same set is registered in the storage position of the encrypted value a' of the first table 143 and the storage position of the encrypted value b' of the second table 144.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-145475
(P2004-145475A)
(43)公開日　平成16年5月20日(2004.5.20)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 15/00	G06F	15/00	330B	5B035
G06F 12/00	G06F	12/00	537A	5B058
G06F 17/60	G06F	17/60	140	5B072
G06K 7/00	G06F	17/60	512	5B082
G06K 7/10	G06K	7/00	U	5B085

審査請求 未請求　請求項の数 27　ＯＬ　（全 34 頁）　最終頁に続く

(21)出願番号　特願2002-307471(P2002-307471)
(22)出願日　平成14年10月22日(2002.10.22)

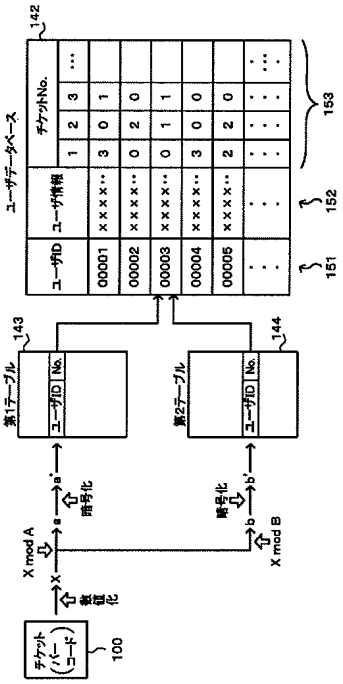
(71)出願人　501374714
パテントワン株式会社
東京都渋谷区渋谷３丁目１７番４号
(74)代理人　100104916
弁理士　古溝　聡
(72)発明者　鵜川　太郎
東京都板橋区前野町２－３３－１５　エスポワール常盤台２０７号
(72)発明者　古溝　聡
東京都北区十条仲原４－１－１　レールシティ十条清水坂公園５０９号

Ｆターム(参考)　5B035 AA13 BB01 BB09 CA06
5B058 CA40 KA02 KA04 KA31 KA35 YA20
5B072 BB00 CC08 CC24 MM01 MM11

最終頁に続く

(54)【発明の名称】識別情報発行システム及び方法、識別情報認証システム及び方法、並びにプログラム

(57)【要約】
【課題】識別情報の認証処理の高速化とセキュリティの向上とを同時に達成すると共に、処理量を増大させることなく、各ユーザが複数の識別情報を使い分けられる。
【解決手段】ユーザＩＤ及びチケットＮｏ．を含む発行要求があると、ランダムなパターンのチケットを生成し、これを数値化する。この数値を除数Ａ、Ｂで除算した剰余ａ、ｂを求め、これらをさらに暗号化した暗号化値ａ’、ｂ’を生成する。第１テーブル１４３の暗号化値ａ’の記憶位置と第２テーブル１４４の暗号化値ｂ’の記憶位置に、同一の組が登録されていなければ、発行要求に含まれるユーザＩＤ及びチケットＮｏ．の組を登録し、チケットを要求元に送信する。送信したチケットが入力されると、同様にして暗号化値ａ’、ｂ’が生成され、第１テーブル１４３の暗号化値ａ’の記憶位置と第２テーブル１４４の暗号化値ｂ’の記憶位置に同一の組が登録されていれば、チケットを認証する。
【選択図】　図４



【特許請求の範囲】
【請求項１】
１人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行システムであって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段と、
前記発行要求受信手段による発行要求の受信に応答して、識別情報を生成する識別情報生成手段と、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段と、
前記数値組に含まれる複数の数値にそれぞれ対応して用意された複数のテーブルと、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段と、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する組み合わせ登録手段と、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせて登録された後に、前記識別情報生成手段が生成した識別情報を、前記発行要求したユーザに送信する識別情報送信手段と
を備えることを特徴とする識別情報発行システム。
【請求項２】
前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段をさらに備える
ことを特徴とする請求項１に記載の識別情報発行システム。
【請求項３】
前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段と、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段とをさらに備える
ことを特徴とする請求項１または２に記載の識別情報発行システム。
【請求項４】
前記識別情報送信手段がユーザに送信した識別情報を入力する識別情報入力手段を含むコンピュータ装置に接続され、
前記コンピュータ装置は、
前記識別情報入力手段から入力された識別情報に基づいて、前記数値組生成手段と同様の方法により、該入力された識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成する第２の数値組生成手段と、
前記第２の数値組生成手段が生成した数値組を前記識別情報発行システムに送信する数値組送信手段とを備え、
前記識別情報発行システムは、前記数値組送信手段から送信された数値組を受信する数値組受信手段をさらに備え、
前記組み合わせ抽出手段は、前記数値組受信手段が受信した数値組に含まれるそれぞれの

数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する
ことを特徴とする請求項３に記載の識別情報発行システム。
【請求項５】
前記数値組生成手段は、
前記識別情報を所定の方法により数値化し、該識別情報と１対１で対応した数値を生成する数値生成手段と、
前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余を算出し、各剰余を前記数値組に含まれる複数の数値とする剰余算出手段とを備え、
前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きい
ことを特徴とする請求項１乃至４のいずれか１項に記載の識別情報発行システム。
【請求項６】
前記数値組生成手段は、
前記識別情報を所定の方法により数値化し、該識別情報と１対１で対応した数値を生成する数値生成手段と、
前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余をそれぞれ算出する剰余算出手段と、
前記剰余算出手段が算出した各剰余を予め用意された暗号鍵を用いて暗号化した暗号化値を生成し、各暗号化値を前記数値組に含まれる複数の数値とする暗号化値生成手段とを備え、
前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きい
ことを特徴とする請求項１乃至４のいずれか１項に記載の識別情報発行システム。
【請求項７】
前記各剰余を暗号化するための暗号鍵は、復号鍵とは非対称の暗号鍵である
ことを特徴とする請求項６に記載の識別情報発行システム。
【請求項８】
前記数値生成手段が生成した数値を予め用意された暗号鍵を用いて暗号化する暗号化手段をさらに備え、
前記剰余算出手段は、前記暗号化手段が算出した剰余を前記複数の除数で除算した剰余をそれぞれ算出する
ことを特徴とする請求項５乃至７のいずれか１項に記載の識別情報発行システム。
【請求項９】
前記数値を暗号化するための暗号鍵は、復号鍵とは非対称の暗号鍵である
ことを特徴とする請求項８に記載の識別情報発行システム。
【請求項１０】
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報のキャンセル要求を受信するキャンセル要求受信手段と、
前記キャンセル要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段とをさらに備える
ことを特徴とする請求項１乃至９のいずれか１項に記載の識別情報発行システム。
【請求項１１】
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の再発行要求を受信する再発行要求受信手段と、
前記再発行要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段と、
前記組み合わせ削除手段がユーザを示す情報と識別情報の種別との組み合わせを各テーブルから削除した後に、前記識別情報生成手段による識別情報の生成、前記数値組生成手段

による数値組の生成、前記登録判別手段による組み合わせの登録の判別、前記組み合わせ登録手段によるユーザを示す情報と識別情報の種別との組み合わせの登録、及び前記識別情報送信手段による識別情報の送信を、再度実行させる識別情報再発行手段とをさらに備える
ことを特徴とする請求項１乃至１０のいずれか１項に記載の識別情報発行システム。
【請求項１２】
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行予約を受信する発行予約受信手段と、
前記発行予約受信手段が受信した識別情報の発行予約を、該発行予約と共に受信したユーザを示す情報及び識別情報の種別に関連付けて登録する発行予約登録手段とをさらに備え、
前記識別情報生成手段は、前記発行要求受信手段が識別情報の発行要求と共に受信したユーザを示す情報及び識別情報の種別に関連付けて、前記発行予約登録手段に発行予約が登録されているときに、識別情報を生成する
ことを特徴とする請求項１乃至１１のいずれか１項に記載の識別情報発行システム。
【請求項１３】
前記発行要求受信手段は、ユーザが有する携帯端末装置から、該携帯端末装置固有の識別情報と共に、ユーザからの識別情報の発行要求を受信し、
前記識別情報発行システムは、前記識別情報生成手段が生成した識別情報を、前記発行要求受信手段が前記発行要求と共に受信した携帯端末装置固有の識別情報を暗号鍵として用いて暗号化する識別情報暗号化手段をさらに備え、
前記識別情報送信手段は、前記識別情報暗号化手段が暗号化した識別情報を前記発行要求を送信した携帯端末装置に送信し、
前記識別情報送信手段から送信された暗号化された識別情報は、該識別情報を受信した携帯端末装置において、該携帯端末装置固有の識別情報を復号鍵として復号化される
ことを特徴とする請求項１乃至１２のいずれか１項に記載の識別情報発行システム。
【請求項１４】
前記識別情報は、一義的に特定可能な画像パターンによって構成される
ことを特徴とする請求項１乃至１３のいずれか１項に記載の識別情報発行システム。
【請求項１５】
１人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証システムであって、
ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と１対１で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録した複数のテーブルと、
識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段と、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段と
を備えることを特徴とする識別情報認証システム。
【請求項１６】
前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録し、該ユーザに発行した後に破棄されている

ことを特徴とする請求項１５に記載の識別情報認証システム。
【請求項１７】
前記識別情報は、一義的に特定可能な画像パターンによって構成される
ことを特徴とする請求項１５または１６に記載の識別情報認証システム。
【請求項１８】
１人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行方法であって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信するステップと、
前記発行要求の受信に応答して、識別情報を生成するステップと、
前記生成した識別情報に基づいて、該生成した識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成するステップと、
前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するステップと、
前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別するステップと、
同一の組み合わせが登録されていないと判別したときに、前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録するステップと、
各テーブルにユーザを示す情報と識別情報の種別とが組み合わせて登録された後に、前記生成した識別情報を発行要求をしたユーザに送信するステップと
を含むことを特徴とする識別情報発行方法。
【請求項１９】
前記生成した識別情報が送信された後、該識別情報を破棄するステップをさらに含む
ことを特徴とする請求項１８に記載の識別情報発行方法。
【請求項２０】
前記ユーザに送信された識別情報に基づいて、前記生成された識別情報に基づいて数値組を生成するのと同様の方法により生成され、該送信された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、
ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、
全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証するステップとをさらに含む
ことを特徴とする請求項１８または１９に記載の識別情報発行方法。
【請求項２１】
１人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証方法であって、
ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と１対１で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する複数のテーブルを予め準備するステップと、
識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、
ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、
全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザから提

示された識別情報を認証するステップと
を含むことを特徴とする識別情報認証方法。
【請求項２２】
前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録し、該ユーザに発行した後に破棄されている
ことを特徴とする請求項２１に記載の識別情報認証方法。
【請求項２３】
１人のユーザが複数の種別を使い分けられるようにした識別情報を発行するためのプログラムであって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段、
前記発行要求受信手段による発行要求の受信に応答して、識別情報を生成する識別情報生成手段、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段、
前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するテーブル準備手段、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する組み合わせ登録手段、及び、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせて登録された後に、前記識別情報生成手段が生成した識別情報を発行要求をしたユーザに送信する識別情報送信手段
としてコンピュータ装置を機能させるためのプログラム。
【請求項２４】
前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段
として前記コンピュータ装置をさらに機能させることを特徴とする請求項２３に記載のプログラム。
【請求項２５】
前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段
として前記コンピュータ装置をさらに機能させることを特徴とする請求項２３または２４に記載のプログラム。
【請求項２６】
１人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証するためのプログラムであって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と１対１で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する複数のテーブルを準備するテーブル準備手段、
識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段
としてコンピュータ装置を機能させるためのプログラム。
【請求項２７】
前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録し、該ユーザに発行した後に破棄されている
ことを特徴とする請求項２６に記載のプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、イベントのチケットなどとして用いられる識別情報の発行及び認証に関するものである。
【０００２】
【従来の技術】
近年、携帯電話技術は、急速に進歩しており、Ｗｅｂ接続機能を有するものが一般的となり、また、表示装置の解像度も高くなっている。このような携帯電話技術の進歩に伴って、コンサートなどのイベントのチケットを携帯電話機上に表示されるバーコードによって構成し、Ｗｅｂ接続サービスを利用して配信するものが登場している。
【０００３】
携帯電話機に配信されたバーコードは、イベント会場の入口に設置されたコンピュータ装置が有するバーコードリーダによって読み取られ、これを発行した（管理する）サーバ装置に送られるものとなる。サーバ装置は、送られてきたバーコードが正当であるかどうかを認証し、正当なものであると認証できれば、その旨を入口のコンピュータ装置に通知するものとなる。この通知に従って、チケットとしてのバーコードを購入したユーザが、イベント会場に入場することが認められる。
【０００４】
従来では、サーバ装置は、バーコードを発行して携帯電話機に配信すると共に、そのバーコードを内部のデータベースに保存するものとしていた。携帯電話機に表示されたバーコードがバーコードリーダによって読み取られて送られてくると、サーバ装置は、送られてきたバーコードを保存しておいたバーコードと照合することによって、そのバーコードが正当なものであることを認証するものとしていた（例えば、特許文献１参照）。
【０００５】
【特許文献１】
特許第３２０７１９２号公報
【０００６】
【発明が解決しようとする課題】
しかしながら、特許文献１の技術では、ユーザに発行された認証情報としてのバーコードは、少なくともそのバーコードを用いて認証を行うことが不要となるまで、サーバ装置内

に継続的に置かれることとなる。すると、サーバ装置がハッキングされることによって、認証情報であるバーコードが漏洩するという危険が非常に大きかった。

【０００７】

認証情報としてのバーコードの漏洩は、サーバ装置内においてバーコードを暗号化して保存しておくことによって防止を図ることができる。しかし、バーコードを暗号化して保存しておくことにより、認証を行う際に暗号化したバーコードの復号化が必要となり、認証に要する処理が増大してしまう。

【０００８】

暗号強度を低くすれば、認証に要する処理の増大は抑えられるが、暗号の解読によってバーコードが漏洩する危険は高くなる。逆に暗号強度を高くすれば、暗号の解読が困難であるためバーコードが漏洩する危険は低く抑えられるが、認証の際におけるバーコードの復号化が非常に複雑なものとなり、認証に要する処理量が大きくなってしまう。このように、特許文献１の技術では、認証処理の高速化とセキュリティの向上とを同時に達成することができなかった。

【０００９】

ところで、コンサートなどのイベント、特に人気が高く、キャパシティが大きい会場でのイベントとなると、その開場時間から開始時間までの短い時間（例えば、１時間程度）において、数万人程度の人がイベント会場に入場しようとする。イベントのチケットとして携帯電話機に表示されたバーコードを使用した場合、膨大な数のバーコードの認証処理を短時間の間で行わなければならない。

【００１０】

十分なセキュリティを確保すべくサーバ装置内のバーコードを暗号化していた場合には、イベントの開場時間から開始時間までの短い時間での処理量が非常に大きなものとなる。入場時の混乱を避けるためには、サーバ装置のダウンは絶対的に避けなければならないので、非常に処理能力が大きいサーバ装置を用意しておかなければならない。一方、開場時間より前や、開始時間よりも後になると、サーバ装置において行われる処理はあまりない。すると、短期的にサーバ装置の稼働率が高くなるときはあっても、平均の稼働率は低いものにとどまっており、サーバ装置の処理能力を十分に生かし切れない。

【００１１】

また、特許文献１では、１人のユーザが認証情報として使用するバーコードは１つだけであることを前提としているが、コンサートなどのイベントのチケットとしてバーコードを使用する場合には、１人のユーザに複数のバーコードを使用させる必要がある。１人のユーザが複数のバーコードを使用する場合、認証の際にバーコードの照合を行わなければならない回数は、ユーザの数ではなく、最大でバーコードの数だけ、平均でもバーコードの数の半分となる。すると、１人のユーザが使用できるバーコードの数が多くなればなるほど、処理量も増大してしまうという問題があった。

【００１２】

本発明は、識別情報の発行及び認証において、認証処理の高速化とセキュリティの向上とを同時に達成することができる識別情報発行システム等を提供することを目的とする。

【００１３】

本発明は、また、識別情報の発行及び認証において、１人のユーザが複数の識別情報を使い分けても、処理量をあまり増大させることがない識別情報発行システム等を提供することを目的とする。

【００１４】

【課題を解決するための手段】

上記目的を達成するため、本発明の第１の観点にかかる識別情報発行システムは、

１人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行システムであって、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段と、

前記発行要求受信手段による発行要求の受信に応答して、識別情報を生成する識別情報生成手段と、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段と、
前記数値組に含まれる複数の数値にそれぞれ対応して用意された複数のテーブルと、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段と、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する組み合わせ登録手段と、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせて登録された後に、前記識別情報生成手段が生成した識別情報を、前記発行要求したユーザに送信する識別情報送信手段と
を備えることを特徴とする。

【００１５】

上記識別情報発行システムは、
前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段をさらに備えるものとすることができる。

【００１６】

上記識別情報発行システムでは、識別情報生成手段が生成した識別情報に基づいて数値組が求められ、数値組に含まれる複数の数値に対応した各テーブルの記憶位置にユーザを示す情報と識別情報の種別とが組み合わせて登録される。このように識別情報に応じて記憶位置を定めて各テーブルへの登録を行うことにより、後述するように識別情報の認証を行う際に、識別情報同士を照合する必要がなくなる。このため、識別情報生成手段が生成した識別情報が識別情報送信手段によりユーザに送信された後は、上記識別情報発行システム内に識別情報そのものを残しておく必要がなく、識別情報破棄手段によって破棄してしまってもよい。

【００１７】

上記識別情報発行システムは、内部に識別情報そのものが残っていないので、仮にハッカーに侵入されても各ユーザの識別情報が盗み出されることがなく、高度のセキュリティを達成することができる。また、テーブルのための記憶容量は必要となるが、識別情報そのもののための記憶容量は必要ないので、特に識別情報の情報量が大きいときには、システムに必要な記憶容量も小さくすることができる。さらに、テーブルには、ユーザを示す情報と識別情報の種別とを組み合わせて登録するため、後述するように１人のユーザが複数の識別情報を使い分ける場合において、識別情報の種別までを認証できるようになる。

【００１８】

なお、数値組生成手段が数値組を生成するために用いる識別情報と、識別情報送信手段がユーザに送信する識別情報とは、完全に一致したものとは限らない。例えば、識別情報生成手段は、まず特定の数値を生成し、この数値から数値組生成手段が数値組を生成するものとし、識別情報送信手段は、前記特定の数値から双方向で一義的に定められる特定の情報を送信するものとしてもよい。前記特定の数値と前記特定の情報とは、ここでは、実質的な内容としては同じ識別情報であると見ることができる。

【００１９】

上記識別情報発行システムは、
前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ

抽出手段と、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段とをさらに備えるものとすることができる。
【００２０】
このような構成を備えることにより、組み合わせ抽出手段が各テーブルからユーザを示す情報と識別情報の種別との組み合わせを抽出し、組み合わせ判定手段が同一の組み合わせが抽出されたかどうかを判定すれば、識別情報の認証を行える。各テーブルには識別情報の種別まで登録されているので、ユーザだけでなく種別の認証も行える。
【００２１】
ここで行う認証の処理は、各テーブルに登録されているユーザを示す情報と識別情報の種別の抽出と、その比較だけでよいので、識別情報同士を照合する場合に比べて高速な処理が行える。識別情報の照合ではないので、システム内部に残した識別情報の復号化といった処理量を増大させる処理も必要ない。しかも、発行した識別情報の数が増加しても、処理量の増加はそれよりもずっと少ない。従って、１人のユーザが複数の種別の識別情報を使い分けるものとしても、認証処理の処理量があまり増大しない。
【００２２】
この場合において、上記識別情報発行システムは、
前記識別情報送信手段がユーザに送信した識別情報を入力する識別情報入力手段を含むコンピュータ装置に接続されていてもよい。ここで、
前記コンピュータ装置は、
前記識別情報入力手段から入力された識別情報に基づいて、前記数値組生成手段と同様の方法により、該入力された識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成する第２の数値組生成手段と、
前記第２の数値組生成手段が生成した数値組を前記識別情報発行システムに送信する数値組送信手段とを備えるものとすることができ、
前記識別情報発行システムは、前記数値組送信手段から送信された数値組を受信する数値組受信手段をさらに備えるものとすることができる。そして、
前記組み合わせ抽出手段は、前記数値組受信手段が受信した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するものとすることができる。
【００２３】
この場合、ユーザに送信された識別情報に基づいて数値組を生成するまでの処理は、別のコンピュータ装置において行うものとなっている。例えば、識別情報がイベントのチケットなどとして用いられる場合には、短時間の間に処理が集中するが、識別情報の入力から数値組の生成という比較的処理量が大きくなる処理は、分散して行うことができる。
【００２４】
上記識別情報発行システムにおいて、
前記数値組生成手段は、例えば、
前記識別情報を所定の方法により数値化し、該識別情報と１対１で対応した数値を生成する数値生成手段と、
前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余を算出し、各剰余を前記数値組に含まれる複数の数値とする剰余算出手段とを備えるものとすることができる。ここで、
前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きいことが条件となる。
【００２５】
前記数値組生成手段は、また、

前記識別情報を所定の方法により数値化し、該識別情報と１対１で対応した数値を生成する数値生成手段と、
前記数値生成手段が生成した識別情報に対応した数値を、互いに異なる複数の除数で除算した剰余をそれぞれ算出する剰余算出手段と、
前記剰余算出手段が算出した各剰余を予め用意された暗号鍵を用いて暗号化した暗号化値を生成し、各暗号化値を前記数値組に含まれる複数の数値とする暗号化値生成手段とを備えるものとすることができる。ここでも、
前記複数の除数の最小公倍数は、前記識別情報に対応した数値がとり得る値の最大値と最小値との差よりも大きいことが条件となる。

【００２６】

なお、前記各剰余を暗号化するための暗号鍵は、復号鍵とは非対称の暗号鍵であることが好ましい。

【００２７】

さらに、前記数値組生成手段を上記の２通りのいずれかで構成した場合、上記識別情報発行システムは、
前記数値生成手段が生成した数値を予め用意された暗号鍵を用いて暗号化する暗号化手段をさらに備えるものとすることができ、
前記剰余算出手段は、前記暗号化手段が算出した剰余を前記複数の除数で除算した剰余をそれぞれ算出するものとすることができる。

【００２８】

なお、前記数値を暗号化するための暗号鍵も、復号鍵とは非対称の暗号鍵であることが好ましい。

【００２９】

上記のように識別情報生成手段が生成した識別情報から数値組を生成すると、異なる識別情報から生成された数値組では、数値組に含まれる全ての数値が一致することはなくなる。これにより、数値組から識別情報を一義的に定めることができる。識別情報に対応した数値から求めた各剰余を暗号化した暗号化値を、各テーブルへの記憶位置として適用することで、上記識別情報発行システムからテーブルの情報を盗み出し、これを解析しても剰余の値が分からないので、元の識別情報を復元できない。特に暗号鍵として非対称鍵を適用すると、どこにも復号鍵がないので情報を盗み出して復号を行うことができず、元の識別情報の復元は、どのような暗号技術に比べても遜色がないか、それ以上に困難なものとなる。

【００３０】

上記識別情報発行システムは、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報のキャンセル要求を受信するキャンセル要求受信手段と、
前記キャンセル要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段とをさらに備えるものとすることができる。

【００３１】

上記識別情報発行システムは、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の再発行要求を受信する再発行要求受信手段と、
前記再発行要求をしたユーザを示す情報と発行要求された識別情報の種別との組み合わせを、前記複数のテーブルからそれぞれ削除する組み合わせ削除手段と、
前記組み合わせ削除手段がユーザを示す情報と識別情報の種別との組み合わせを各テーブルから削除した後に、前記識別情報生成手段による識別情報の生成、前記数値組生成手段による数値組の生成、前記登録判別手段による組み合わせの登録の判別、前記組み合わせ登録手段によるユーザを示す情報と識別情報の種別との組み合わせの登録、及び前記識別情報送信手段による識別情報の送信を、再度実行させる識別情報再発行手段とをさらに備

えるものとすることもできる。

【００３２】

このような構成を備えるものとすることで、上記識別情報発行システムの内部に発行済みの識別情報が残っていなくても、ユーザは、識別情報のキャンセルや再発行を受けることができるようになる。ところで、識別情報のキャンセルや再発行を行う場合、比較的処理量が多い各テーブルのサーチが必要となっている。識別情報がイベントのチケットなどとして用いられる場合であっても、キャンセルや再発行の要求が短時間に集中することはほとんどあり得ないので、処理量として特に問題になることはない。

【００３３】

上記識別情報発行システムは、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行予約を受信する発行予約受信手段と、

前記発行予約受信手段が受信した識別情報の発行予約を、該発行予約と共に受信したユーザを示す情報及び識別情報の種別に関連付けて登録する発行予約登録手段とをさらに備えるものとすることができる。この場合において、

前記識別情報生成手段は、前記発行要求受信手段が識別情報の発行要求と共に受信したユーザを示す情報及び識別情報の種別に関連付けて、前記発行予約登録手段に発行予約が登録されているときに、識別情報を生成することができる。

【００３４】

識別情報がイベントのチケットなどとして用いられる場合は、申し込み受付を開始してから短時間の間で多くの申し込みがある場合がある。申し込みが集中する時間には、上記したような発行予約登録だけを行うものとすれば、この発行予約登録の処理量は比較的小さいので、上記識別情報発行システムに、必要以上に大きな処理負荷がかかることはない。そして、比較的処理量の大きい識別情報の実際の発行は、発行予約を登録した後に処理を分散して行うことができるようになる。

【００３５】

上記識別情報発行システムにおいて、

前記発行要求受信手段は、ユーザが有する携帯端末装置から、該携帯端末装置固有の識別情報と共に、ユーザからの識別情報の発行要求を受信するものであってもよい。この場合において、

前記識別情報発行システムは、前記識別情報生成手段が生成した識別情報を、前記発行要求受信手段が前記発行要求と共に受信した携帯端末装置固有の識別情報を暗号鍵として用いて暗号化する識別情報暗号化手段をさらに備えるものとすることができ、

前記識別情報送信手段は、前記識別情報暗号化手段が暗号化した識別情報を前記発行要求を送信した携帯端末装置に送信するものとすることができる。この場合において、

前記識別情報送信手段から送信された暗号化された識別情報は、該識別情報を受信した携帯端末装置において、該携帯端末装置固有の識別情報を復号鍵として復号化されるものとすればよい。

【００３６】

この場合、識別情報の発行要求をした携帯端末装置以外では、識別情報が正しく復号されない。このため、識別情報送信手段から送信して携帯端末装置に届くまでの間で識別情報が盗み出されたり、不正な転送があったとしても、正当に識別情報の発行を受けた者以外は、正しい識別情報を得ることができない。これにより、識別情報の不正使用を防ぐことができる。

【００３７】

上記識別情報発行システムにおいて、

前記識別情報は、一義的に特定可能な画像パターンによって構成されるものとすることができる。

【００３８】

識別情報を画像パターンによって構成するものとした場合、従来では、これを記憶してお

くのにかなりの記憶容量が必要となった。また、照合の処理量が大きなものとなっていた。特に複雑な画像パターンを適用したときには、これらの問題が大きくなる。これに対して、上記識別情報発行システムでは、識別情報のための記憶容量や照合の処理が全く必要ないので、識別情報として複雑な画像パターンを適用しても、記憶容量の増大や処理量の増大の問題を発生させることがない。

【００３９】

上記目的を達成するため、本発明の第２の観点にかかる識別情報認証システムは、

１人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証システムであって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と１対１で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録した複数のテーブルと、

識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段と、

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段と、

前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段と

を備えることを特徴とする。

【００４０】

上記識別情報認証システムにおいて、

前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録し、該ユーザに発行した後に破棄されていてもよい。

【００４１】

上記識別情報認証システムでは、組み合わせ抽出手段が各テーブルからユーザを示す情報と識別情報の種別との組み合わせを抽出し、組み合わせ判定手段が同一の組み合わせが抽出されたかどうかを判定すれば、識別情報の認証を行える。各テーブルには識別情報の種別まで登録されているので、ユーザだけでなく種別の認証も行える。

【００４２】

ここで行う認証の処理は、各テーブルに登録されているユーザを示す情報と識別情報の種別の抽出と、その比較だけでよいので、識別情報同士を照合する場合に比べて高速な処理が行える。識別情報の照合ではないので、システム内部に残した識別情報の復号化といった処理量を増大させる処理も必要ない。しかも、発行した識別情報の数が増加しても、処理量の増加はそれよりもずっと少ない。従って、１人のユーザが複数の種別の識別情報を使い分けるものとしても、認証処理の処理量があまり増大しない。

【００４３】

さらに、識別情報同士の照合によって認証を行うのではないので、識別情報そのものを、上記識別情報認証システム内に残しておく必要がなく、各テーブルへの登録が終了し、識別情報をユーザに発行した後には破棄されている。このように内部に識別情報そのものが残っていないので、仮にハッカーに侵入されても各ユーザの識別情報が盗み出されることがなく、高度のセキュリティを達成することができる。また、テーブルのための記憶容量は必要となるが、識別情報そのもののための記憶容量は必要ないので、特に識別情報の情報量が大きいときには、システムに必要な記憶容量も小さくすることができる。

【００４４】

上記識別情報認証システムにおいて、

前記識別情報は、一義的に特定可能な画像パターンによって構成されるものとすることができる。

【００４５】

識別情報を画像パターンによって構成するものとした場合、従来では、これを記憶しておくのにかなりの記憶容量が必要となった。また、照合の処理量が大きなものとなっていた。特に複雑な画像パターンを適用したときには、これらの問題が大きくなる。これに対して、上記識別情報認証システムでは、識別情報のための記憶容量や照合の処理が全く必要ないので、識別情報として複雑な画像パターンを適用しても、記憶容量の増大や処理量の増大の問題を発生させることがない。

【００４６】

上記目的を達成するため、本発明の第３の観点にかかる識別情報発行方法は、１人のユーザが複数の種別を使い分けられるようにした識別情報を発行する識別情報発行方法であって、

ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信するステップと、

前記発行要求の受信に応答して、識別情報を生成するステップと、

前記生成した識別情報に基づいて、該生成した識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成するステップと、

前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するステップと、

前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別するステップと、

同一の組み合わせが登録されていないと判別したときに、前記生成した数値組に含まれるそれぞれの数値に対応した各テーブルに記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録するステップと、

各テーブルにユーザを示す情報と識別情報の種別とが組み合わせて登録された後に、前記生成した識別情報を発行要求をしたユーザに送信するステップと

を含むことを特徴とする。

【００４７】

上記識別情報発行方法は、

前記生成した識別情報が送信された後、該識別情報を破棄するステップをさらに含むものとしてもよい。

【００４８】

上記識別情報発行方法は、

前記ユーザに送信された識別情報に基づいて、前記生成された識別情報に基づいて数値組を生成するのと同様の方法により生成され、該送信された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、

ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、

全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証するステップとをさらに含むものとしてもよい。

【００４９】

上記目的を達成するため、本発明の第４の観点にかかる識別情報認証方法は、１人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証する識別情報認証方法であって、

ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と１対１で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録す

る複数のテーブルを予め準備するステップと、
識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出するステップと、
ユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定するステップと、
全てのテーブルから同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証するステップと
を含むことを特徴とする。

【００５０】
上記識別情報発行方法において、
前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録し、該ユーザに発行した後に破棄されていてもよい。

【００５１】
上記目的を達成するため、本発明の第５の観点にかかるプログラムは、
１人のユーザが複数の種別を使い分けられるようにした識別情報を発行するためのプログラムであって、
ユーザを示す情報及び識別情報の種別と共に、ユーザからの識別情報の発行要求を受信する発行要求受信手段、
前記発行要求受信手段による発行要求に受信に応答して、識別情報を生成する識別情報生成手段、
前記識別情報生成手段が生成した識別情報に基づいて、該生成した識別情報と１対１で対応付けられた数値組であって、複数の数値からなる数値組を生成する数値組生成手段、
前記数値組に含まれる複数の数値にそれぞれ対応する複数のテーブルを予め準備するテーブル準備手段、
前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、ユーザを示す情報と識別情報の種別との組み合わせとして同一の組み合わせが登録されているかどうかを判別する登録判別手段、
前記登録判別手段が同一の組み合わせが登録されていないと判別したときに、前記数値組生成手段が生成した数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置に、前記発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する組み合わせ登録手段、及び、
前記組み合わせ登録手段により各テーブルにユーザを示す情報と識別情報の種別とが組み合わせて登録された後に、前記識別情報生成手段が生成した識別情報を発行要求をしたユーザに送信する識別情報送信手段
としてコンピュータ装置を機能させることを特徴とする。

【００５２】
上記第５の観点にかかるプログラムは、
前記識別情報送信手段により前記識別情報生成手段が生成した識別情報が送信された後、該識別情報を破棄する識別情報破棄手段
として前記コンピュータ装置をさらに機能させるものであってもよい。

【００５３】
上記第５の観点にかかるプログラムは、
前記識別情報送信手段によりユーザに送信された識別情報に基づいて、前記数値組生成手段が数値組を生成するのと同様の方法により生成され、該送信された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、

前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び、
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザに送信された識別情報を認証する認証手段
として前記コンピュータ装置をさらに機能させるものであってもよい。

【００５４】

上記目的を達成するため、本発明の第６の観点にかかるプログラムは、
１人のユーザが複数の種別を発行されて、使い分けられるようにした識別情報を認証するためのプログラムであって、
ユーザからの発行要求に応答して識別情報が生成されたときに、該識別情報と１対１で対応付けられた数値組に含まれる各数値に対応したそれぞれの記憶位置に、該識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録する複数のテーブルを準備するテーブル準備手段、
識別情報を発行されたユーザから提示された識別情報に基づいて、前記テーブルへの登録時と同様の方法により生成され、該提示された識別情報と１対１で対応付けられた数値組に含まれるそれぞれの数値に対応した各テーブルの記憶位置から、登録されているユーザを示す情報と識別情報の種別との組み合わせを抽出する組み合わせ抽出手段、
前記組み合わせ抽出手段が抽出したユーザを示す情報と識別情報の種別との組み合わせとして全てのテーブルから同一の組み合わせが抽出されたかどうかを判定する組み合わせ判定手段、及び
前記組み合わせ判定手段が同一の組み合わせが抽出されたと判定したときに、前記ユーザから提示された識別情報を認証する認証手段
としてコンピュータ装置を機能させることを特徴とする。

【００５５】

上記第６の観点にかかるプログラムにおいて、
前記ユーザからの発行要求に応答して生成された識別情報は、前記複数のテーブルに識別情報の発行要求をしたユーザを示す情報と発行要求された識別情報の種別とを組み合わせて登録し、該ユーザに発行した後に破棄されていてもよい。

【００５６】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態について説明する。

【００５７】

図１は、この実施の形態にかかるチケット発行システムを示すブロック図である。このチケット発行システムは、予め登録したユーザがコンサートやスポーツなどのイベントのチケットを購入し、購入したチケットの認証を受けて、イベント会場に入場できるようにしたものである。チケットが認証されるということは、そのチケットが当該イベントについてのチケットであるということを認証するということである。なお、このチケット発行システムで発行するチケットとしては、二次元バーコードが用いられている。

【００５８】

図示するように、このチケット発行システムは、サーバ装置１と、入場ゲート装置２と、登録したユーザが管理する携帯電話機３とを含んでいる。サーバ装置１及び入場ゲート装置２は、チケット発行者が管理するものであり、両者間は、専用線４で接続されている。携帯電話機３は、Ｗｅｂ接続機能を備えるものであり、携帯電話網６からインターネット５に入り、サーバ装置１に接続できるようになっている。

【００５９】

サーバ装置１は、チケットの発行及び認証を管理するコンピュータ装置である。入場ゲート装置２は、イベント会場の入口に設置されるもので、イベント会場内への人の出入りを規制するものである。入場ゲート装置２は、図では１つだけ示しているが、実際にはイベント会場の入口に複数設置される。携帯電話機３は、サーバ装置１が発行したチケットを

受信し、表示するものである。次に、サーバ装置１、入場ゲート装置２、及び携帯電話機３の詳細について説明するものとする。

【００６０】

図２は、図１のサーバ装置１の構成を示すブロック図である。図示するように、サーバ装置１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１と、主記憶装置１２と、通信装置１３と、補助記憶装置１４とを備えている。補助記憶装置１４には、プログラムファイル１４１、ユーザデータベース１４２、第１テーブル１４３及び第２テーブル１４４が記憶されている。

【００６１】

ＣＰＵ１１は、主記憶装置１２に転送されたプログラムを実行し、後述するように、チケットの予約、販売、キャンセル、再発行、認証などの種々の処理を行う。チケットの構成については後述する。主記憶装置１２は、ＣＰＵ１１の主記憶領域を提供するもので、プログラムファイル１４１のプログラムが転送され、また、ＣＰＵ１１の作業領域として用いられる。通信装置１３は、専用線４を介して入場ゲート装置２と情報を送受信すると共に、インターネット５及び携帯電話網６を介して携帯電話機３と情報を送受信する。

【００６２】

補助記憶装置１４は、ＣＰＵ１１の補助記憶領域を提供するもので、固定ディスク装置などによって構成される。プログラムファイル１４１は、後述するフローチャートに示すプログラムを含むファイルである。ユーザデータベース１４２は、このチケット発行システムを利用してチケットを購入し、そのチケットによる認証を受けて、イベント会場に入場できるユーザに関する情報を登録したデータベースである。第１テーブル１４３及び第２テーブル１４４は、個々のチケットとユーザ及びチケットの種別とを対応付けるために用いられるテーブルである。ユーザデータベース１４２、第１テーブル１４３及び第２テーブル１４４の詳細については後述する。

【００６３】

図３は、このチケット発行システムにおいて適用されるチケットの例を示す図である。図では、携帯電話機３の表示装置に表示された状態を示している。図示するように、このチケット１００は、二階調の二次元バーコードによって構成されており、その四隅には方向チェックマーク１０１～１０４が設けられている。方向チェックマーク１０１～１０４は、チケットの方向を示すもので、１つだけ明表示されるチェックマーク１０４がチケットの右下であることを示している。

【００６４】

チェックマーク１０１～１０４以外のチケット表示部１０５については、チケットＮｏ．とは無関係に、そのパターンを任意に選ぶことができるが、選ばれたパターンは、曖昧性がなく一義的に特定される。もっとも、チケット表示部１０５に特定の情報を含ませるため、一部の特定の場所が特定のパターンを有するものとなっていても構わない。チケット１００の二次元バーコードとしてのパターンは、所定の方法により数値化することができ、パターンと数値とは１対１で対応する。なお、チケット１００のパターンを数値化するプログラムは、サーバ装置１と入場ゲート装置２内に格納されているだけで、外部には公開されていない。

【００６５】

図４は、ユーザデータベース１４２、第１テーブル１４３及び第２テーブル１４４の詳細を示す図である。図示するように、ユーザデータベース１４２は、登録したユーザ毎に、ユーザＩＤ１５１、ユーザ情報１５２、複数のチケット情報１５３を登録したデータベースとなっている。ユーザＩＤ１５１は、各ユーザを一意に識別するための情報であり、チケットの予約や購入などの際には、このユーザＩＤが必要となる。

【００６６】

ユーザ情報１５２は、各ユーザの属性に関する情報を含む。ユーザの属性に関する情報としては、少なくともユーザが設定した（或いはユーザ登録の際に通知された）パスワードと、チケット１００の二次元バーコードを画像データとして携帯電話機３に送信するため

のアドレスを含んでいる。その他、ユーザ情報１５２としては、従来のシステムで適用されてきたような種々の情報を含むものとすることができる。

【００６７】

チケット情報１５３には、イベントの種別（開始日時によっても異なる）毎に固有のチケットＮｏ．に対応して、ユーザのチケットの予約、購入、使用状況を示すフラグが登録されている。フラグの値が０であれば未予約を、１であれば予約済みであるが未購入を、２であれば購入済みであるが未使用（イベント会場に入場していないこと）を、３であれば使用済み（イベント会場に入場したこと）を示している。

【００６８】

第１テーブル１４３及び第２テーブル１４４には、ユーザが何らかのイベントのチケット１００を購入したときに、そのユーザのユーザＩＤ１５１と購入したチケットのチケットＮｏ．との組が、チケット１００のパターンに応じた記憶位置において記憶される。第１テーブル１４３及び第２テーブル１４４からは、ユーザＩＤをキーとしてユーザデータベース１４２を参照することができる。

【００６９】

次に、ユーザＩＤ及びチケットＮｏ．の組が、第１テーブル１４３及び第２テーブル１４４の記憶位置のどこに記憶されるかについて説明する。二次元バーコードからなるチケット１００が発行されると、そのパターンに１対１で対応した整数値となるように数値化される。チケット１００が数値化された数値Ｘは、第１テーブル１４３に対応した除数Ａ（整数値）と、第２テーブル１４４に対応した除数Ｂ（整数値）とで除算され、それぞれの剰余ａ、ｂが求められる。

【００７０】

ここで、除数Ａと除数Ｂとの最小公倍数は、数値Ｘがとりうる最大値Ｘｍａｘと最小値Ｘｍｉｎの差よりも大きいという関係がある。また、除数Ａと除数Ｂとは、互いに素であることが好ましい。この条件を満たす限り、数値Ｘが異なれば、剰余ａと剰余ｂとの両方が一致するということはあり得ない。つまり、異なる数値Ｘに対しては、剰余ａと剰余ｂの組み合わせが全て異なっており、剰余ａと剰余ｂの組み合わせは、チケット１００のパターンと１対１で対応するものとなっている。

【００７１】

剰余ａと剰余ｂとが求められると、それぞれ所定の暗号鍵を用いて暗号化され、暗号化値ａ’、ｂ’が生成される。この暗号鍵は、復号鍵が異なる非対称暗号系の暗号鍵である。また、剰余ａを暗号化する暗号鍵と剰余ｂを暗号化する暗号鍵とは、異なるものであることが好ましい。剰余ａと剰余ｂの組み合わせは、チケット１００のパターンと１対１で対応するので、暗号化値ａ’と暗号化値ｂ’の組み合わせも、チケット１００のパターンと１対１で対応するものとなる。

【００７２】

発行されたチケット１００についてユーザＩＤ及びチケットＮｏ．の組は、第１テーブル１４３の暗号化値ａ’に対応した記憶位置と、第２テーブル１４４の暗号化値ｂ’に対応した記憶位置とに登録されるものとなる。異なるチケット１００であっても、剰余ａ、ｂのいずれか一方が一致することはあるので、同様に暗号化値ａ’、ｂ’のいずれか一方が一致することはある。暗号化値ａ’、ｂ’のいずれか一方が一致していても、ユーザＩＤ及びチケットＮｏ．の組は、第１テーブル１４３及び第２テーブル１４４のいずれか一方において、同じ記憶位置へ重複して登録される（実際には、リストで繋ぐなどの処理が必要となる）。

【００７３】

新たにチケット１００を発行しようとする場合において生成したパターンが、そのチケット１００から求めた暗号化値ａ’に対応する第１テーブル１４３の記憶位置から取り出したユーザＩＤ及びチケットＮｏ．の組と、暗号化値ｂ’に対応する第２テーブル１４４の記憶位置から取り出したユーザＩＤ及びチケットＮｏ．の組とが一致すれば、そのチケット１００は発行済みのものであることが分かる。この場合は、別のパターンが生成される

。

【００７４】

また、ユーザが購入したチケット１００を使ってイベント会場に入場しようとするときは、後述するように入場ゲート装置２においてユーザが購入したチケット１００（携帯電話機３に表示された二次元バーコード）が読み取られるが、読み取られたチケット１００からも同様にして暗号化値ａ’と暗号化値ｂ’とが求められる。

【００７５】

求めた暗号化値ａ’に対応する第１テーブル１４３の記憶位置から取り出したユーザＩＤ及びチケットＮｏ．の組と、暗号化値ｂ’に対応する第２テーブル１４４の記憶位置から取り出したユーザＩＤ及びチケットＮｏ．の組を比較する。両者が一致して、かつチケットＮｏ．が該当するイベントのものを示すときには、チケット１００が正当なものと認証され、ユーザがイベント会場に入場できるようになる。

【００７６】

図５は、図１の携帯電話機３の構成を示すブロック図である。図示するように、携帯電話機３は、ＣＰＵ３１と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）３２と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）３３と、入力装置３４と、表示装置３５と、通信装置３６とを備えている。携帯電話機３は、このほかにも通話を行うために必要な構成要素を備えているが、本発明とは直接関係がないため、図５において省略している。

【００７７】

ＣＰＵ３１は、ＲＯＭ３２に記憶されたプログラムを実行し、サーバ装置１から受信したチケットを管理する処理を行う。ＣＰＵ３１は、入力装置３４からの入力に従って、チケット（二次元バーコード）を表示装置３５に表示させる。ＲＯＭ３２は、ＣＰＵ３１の処理プログラムを記憶する。また、携帯電話機３の個体番号が格納されている。ＲＡＭ３３は、データの記憶領域として用いられるものであり、当該データの中には、チケットの画像データも含まれる。

【００７８】

入力装置３４は、「１」～「０」までの数字キー、「＊」キー、「＃」キーなどを含み、利用者の操作によって必要な情報をＣＰＵ３１に入力する。表示装置３５は、液晶表示装置などによって構成され、チケット（二次元バーコード）の画像を含む種々の情報を表示する。通信装置３６は、インターネット５及び携帯電話網６を介してサーバ装置１と情報を送受信する。

【００７９】

図６は、図１の入場ゲート装置２の構成を示すブロック図である。図示するように、入場ゲート装置２は、ＣＰＵ２１と、記憶装置（主記憶装置及び補助記憶装置を含む）２２と、通信装置２３と、バーコードリーダ２４と、入場ゲート２５と、アラーム装置２６とを備えている。

【００８０】

ＣＰＵ２１は、記憶装置２２に記憶されたプログラムを実行し、携帯電話機３から読み取ったチケットに従ってサーバ装置１から送られてくる通知に従って、ゲートを開放させる、またはアラームを発報させるなどの処理を行う。記憶装置２２は、ＣＰＵ２１の処理プログラムを記憶すると共に、データの記憶領域として用いられる。通信装置２３は、インターネット５を介してサーバ装置１と情報を送受信する。

【００８１】

バーコードリーダ２４は、携帯電話機３の表示装置３５に表示されたチケット（二次元バーコード）の画像を読み取る。入場ゲート２５は、イベント会場の外側から内側に向けて一方向で開放するように構成されており、サーバ装置１から送られてくる通知に従って開放状態となり、ユーザが通過できるようになる。アラーム装置２６は、サーバ装置１から送られてくる通知に従って、不正なチケットがあった旨のアラームを発報する。

【００８２】

なお、サーバ装置１のプログラムファイル１４１に置かれているプログラム、入場ゲート

装置２の記憶装置に記憶されているプログラムは、いずれもオブジェクトコードで記述されたものであって、ソースコードで記述されたプログラムがサーバ装置１及び入場ゲート装置２には置かれていない。

【００８３】

以下、この実施の形態にかかるチケット発行システムにおける処理ついて説明する。この実施の形態にかかるチケット発行システムを利用して、二次元バーコードからなるチケットを購入しようとする者は、予めユーザ登録を行って、ユーザデータベース１４２に登録しておく必要がある。もっとも、ユーザ登録の方法は、従来の方法と変わりがないので、ここではユーザ登録が予めなされているものとし、以下の処理説明におけるユーザとは、ユーザ登録をしたユーザのことである。

【００８４】

新たなイベントについてチケットの販売を行う場合、その予約受付を行うまでに当該チケットについてチケットＮｏ．が付与され、ユーザデータベース１４２にフラグ領域が設定され、その全てに０が設定されることとなる。新たなイベントについてチケットの販売を行う場合は、メールなどによってチケットＮｏ．と共に販売開始がユーザに告知される。なお、チケットの購入に伴う課金やキャンセルに伴う返金なども行われるが、これらの処理は本発明と関係がないので説明を省略する。

【００８５】

ユーザは、チケットを購入する前段階として、ユーザはチケットの購入予約を行う。購入予約ができたユーザは、その予約に基づいてチケットの発行を受け、これを購入する。チケットを購入した後に、ユーザがそれをキャンセルする場合や、チケットをなくして再発行を受ける場合もある。そして、イベント会場の開場時間となると、ユーザが購入したチケットの認証を受け、イベント会場へと入場することとなる。

【００８６】

つまり、この実施の形態にかかるチケット発行システムで行われる処理は、

（１）チケット予約処理
（２）チケット購入処理
（３）チケットキャンセル処理
（４）チケット再発行処理
（５）チケット認証処理

の５つに大きく分けられることとなる。以下、それぞれについて詳しく説明する。

【００８７】

図７は、チケット予約処理を示すフローチャートである。チケットを購入予約しようとするユーザは、まず、自己の携帯電話機３の入力装置３４から、ユーザＩＤとパスワードとを入力する。また、購入予約しようとするチケットのチケットＮｏ．を入力装置３４から入力する（ステップＳ１０１）。さらにユーザが入力装置３４から購入予約の要求を入力すると、ステップＳ１０１で入力されたユーザＩＤ、パスワード及びチケットＮｏ．と共に予約要求が通信装置３６からサーバ装置１に送信される（ステップＳ１０２）。その後、ＣＰＵ３１は、サーバ装置１からの情報の受信待ちとなる。

【００８８】

サーバ装置１では、通信装置１３が携帯電話機３から送られてきた予約要求を受信する（ステップＳ１５１）。この予約要求を受信すると、ＣＰＵ１１は、受信した予約要求に含まれるユーザＩＤがユーザデータベース１４２に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかも判定する（ステップＳ１５２）。

【００８９】

ユーザＩＤが登録されていて、パスワードも正しい場合は、ＣＰＵ１１は、受信した予約要求に含まれるチケットＮｏ．のチケットが予約受付可能であるかどうか、すなわち予約受付を開始したチケットであって、売り切れとなっていないチケットであるかどうかを判定する（ステップＳ１５３）。予約受付可能であれば、ＣＰＵ１１は、当該予約要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグを未

予約を示す０から予約済みを示す１に更新する（ステップＳ１５４）。

【００９０】

フラグの更新が終了すると、ＣＰＵ１１は、予約要求をした携帯電話機３に宛てたメールで、通信装置１３から予約完了通知を送信させる（ステップＳ１５５）。また、予約要求に含まれるユーザＩＤが登録されていないかパスワードが間違っていた場合、或いは予約要求に含まれるチケットＮｏ．のチケットが予約受付不可であった場合には、ＣＰＵ１１は、予約要求をした携帯電話機３に宛てたメールで、通信装置１３から予約不可通知を送信させる（ステップＳ１５６）。予約完了通知または予約不可通知の送信により、サーバ装置１の側における処理は終了となる。

【００９１】

携帯電話機３では、通信装置３６がステップＳ１５５で送信された予約完了通知またはステップＳ１５６で送信された予約不可通知を受信する（ステップＳ１０３）。ＣＰＵ３１は、受信した予約完了通知または予約不可通知を表示装置３５に表示させて、ユーザに示す（ステップＳ１０４）。これで、チケット予約処理が終了する。

【００９２】

図８は、チケット購入処理を示すフローチャートである。チケット購入処理においても、ユーザは、自己の携帯電話機３の入力装置３４から、ユーザＩＤとパスワードとを入力する。また、予約したチケットのうちから購入しようとするチケットのチケットＮｏ．を入力装置３４から入力する（ステップＳ２０１）。さらにユーザが入力装置から購入の要求を入力すると、ステップＳ２０１で入力されたユーザＩＤ、パスワード及びチケットＮｏ．と共に購入要求が通信装置３６からサーバ装置１に送信される（ステップＳ２０２）。その後、ＣＰＵ３１は、サーバ装置１からの情報の受信待ちとなる。

【００９３】

サーバ装置１では、通信装置１３が携帯電話機３から送られてきた購入要求を受信する（ステップＳ２５１）。この購入要求を受信すると、ＣＰＵ１１は、受信した購入要求に含まれるユーザＩＤがユーザデータベース１４２に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかも判定する（ステップＳ２５２）。

【００９４】

ユーザＩＤが登録されていて、パスワードも正しい場合には、ＣＰＵ１１は、受信した購入要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグの状態がチケットの予約済みを示す１になっているかどうかを判定する（ステップＳ２５３）。

【００９５】

フラグの状態がチケットの予約済みを示す１になっていれば、ＣＰＵ１１は、ランダムにパターンを決定して二次元バーコードからなるチケット１００を生成する（ステップＳ２５４）。ＣＰＵ１１は、生成したチケットが既に発行済みのチケット（後述するように使用不能とされたものを含まない）のパターンと同じであるかどうかをチェックする発行済みチケットチェック処理を行う（ステップＳ２５５）。

【００９６】

図９（ａ）は、ステップＳ２５５の発行済みチケットチェック処理を詳細に示すフローチャートである。発行済みチケット生成処理では、ＣＰＵ１１は、ステップＳ２５４で生成したチケットのパターンに対応した数値Ｘを生成する（ステップＳ３０１）。さらに、ＣＰＵ１１は、チケットを数値化した数値Ｘを除数Ａで除算して剰余ａを求め、また、数値Ｘを除数Ｂで除算して剰余ｂを求める（ステップＳ３０２）。

【００９７】

ＣＰＵ１１は、求めた剰余ａを所定の暗号鍵を用いて暗号化して暗号化値ａ’を生成し、また、剰余ｂも同様に暗号化して暗号化値ｂ’を生成する（ステップＳ３０３）。暗号化値ａ’、ｂ’が生成されると、ＣＰＵ１１は、暗号化値ａ’、ｂ’を用いて第１テーブル１４３及び第２テーブル１４４をそれぞれ参照することにより、ステップＳ３０１で数値化したチケットが発行済みのものであるかどうかをチェックするテーブルチェック処理を

行う（ステップＳ３０４）。

【００９８】

図９（ｂ）は、ステップＳ３０４のテーブルチェック処理を詳細に示すフローチャートである。テーブルチェック処理では、ＣＰＵ１１は、第１テーブル１４３の暗号化値ａ’に対応する記憶位置に登録されているユーザＩＤ及びチケットＮｏ．の組を取り出す（ステップＳ３１１）。また、第２テーブル１４４の暗号化値ｂ’に対応する記憶位置に登録されているユーザＩＤ及びチケットＮｏ．の組を取り出す（ステップＳ３１２）。

【００９９】

ＣＰＵ１１は、こうして第１テーブル１４３及び第２テーブル１４４からユーザＩＤ及びチケットＮｏ．の組を取り出すと、両者を比較し、ユーザＩＤとチケットＮｏ．とのいずれもが一致するかどうかを判定する（ステップＳ３１３）。一致していれば、ＣＰＵ１１は、一致を示す情報を返却して（ステップＳ３１４）、テーブルチェック処理を終了し、発行済みチケットチェック処理に復帰する。一致していなければ、ＣＰＵ１１は、不一致を示す情報を返却して（ステップＳ３１５）、テーブルチェック処理を終了し、発行済みチケットチェック処理に復帰する。

【０１００】

図９（ａ）の発行済みチケットチェック処理に復帰すると、ＣＰＵ１１は、テーブルチェック処理から返却された情報が一致を示す情報か不一致を示す情報であるかを判定する（ステップＳ３０５）。不一致を示す情報であったならば、ステップＳ３０３で生成した暗号化値ａ’、ｂ’と共にチケットが未発行を示す情報を返却して（ステップＳ３０６）、発行済みチケットチェック処理を終了し、図８のチケット購入処理に復帰する。一致を示す情報であったならば、発行済みを示す情報を返却して（ステップＳ３０７）、発行済みチケットチェック処理を終了し、図８のチケット購入処理に復帰する。

【０１０１】

図８のチケット購入処理に復帰すると、ＣＰＵ１１は、発行済みチケットチェック処理において未発行が返却されたかどうかを判定する（ステップＳ２５６）。発行済みが返却されていた場合には、ステップＳ２５４の処理に戻り、別のパターンを有する二次元バーコードからなるチケット１００を生成する。

【０１０２】

発行済みが返却されていた場合には、ＣＰＵ１１は、共に返却された暗号化値ａ’に対応する第１テーブル１４３の記憶位置と、暗号化値ｂ’に対応する第２テーブル１４４の記憶位置とに、購入要求と共に受信したユーザＩＤとチケットＮｏ．とを組にして登録する（ステップＳ２５７）。ＣＰＵ１１は、さらに当該購入要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグを予約済みを示す１から購入済みを示す２に更新する（ステップＳ２５８）。

【０１０３】

フラグの更新が終了すると、ＣＰＵ１１は、購入要求をした携帯電話機３に宛てたメールで、通信装置１３から発行したチケットの二次元バーコードの画像データを送信させる（ステップＳ２５９）。チケットの画像データを携帯電話機３に送信した後、ＣＰＵ１１は、当該チケットの画像データをサーバ装置１内に残さないように破棄する（ステップＳ２６０）。チケットを送信し、これを破棄することにより、サーバ装置１の側における処理は終了となる。

【０１０４】

また、購入要求に含まれるユーザＩＤが登録されていないかパスワードが間違っていた場合、或いは購入要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するフラグが予約済みを示していなかった場合には、ＣＰＵ１１は、購入要求をした携帯電話機３に宛てたメールで、通信装置１３から購入不可通知を送信させる（ステップＳ２６１）。購入不可通知の送信により、サーバ装置１の側における処理は終了となる。

【０１０５】

携帯電話機３では、通信装置３６がステップＳ２５９で送信されたチケットまたはステッ

プＳ２６１で送信された購入不可通知を受信する（ステップＳ２０３）。ＣＰＵ３１は、受信したチケットまたは購入不可通知を表示装置３５に表示させて、ユーザに示す（ステップＳ２０４）。これで、チケット購入処理が終了する。なお、ここで受信したチケットは、ユーザが入力装置３４から所定の操作を行うことで、いつでも表示装置３５に表示させることができる。

【０１０６】

図１０は、チケットキャンセル処理を示すフローチャートである。チケットキャンセル処理においても、ユーザは、自己の携帯電話機３の入力装置３４から、ユーザＩＤとパスワードとを入力する。また、購入したチケットのうちからキャンセルしようとするチケットのチケットＮｏ．を入力装置３４から入力する（ステップＳ４０１）。さらにユーザが入力装置３４からキャンセルの要求を入力すると、ステップＳ４０１で入力されたユーザＩＤ、パスワード及びチケットＮｏ．と共にキャンセル要求が通信装置３６からサーバ装置１に送信される（ステップＳ４０２）。その後、ＣＰＵ３１は、サーバ装置１からの情報の受信待ちとなる。

【０１０７】

サーバ装置１では、通信装置１３が携帯電話機３から送られてきたキャンセル要求を受信する（ステップＳ４５１）。このキャンセル要求を受信すると、ＣＰＵ１１は、受信したキャンセル要求に含まれるユーザＩＤがユーザデータベース１４２に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかも判定する（ステップＳ４５２）。

【０１０８】

ユーザＩＤが登録されていて、パスワードも正しい場合には、ＣＰＵ１１は、受信したキャンセル要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグの状態がチケットの購入済みを示す２になっているかどうかを判定する（ステップＳ４５３）。

【０１０９】

フラグの状態が購入済みを示す２になっていれば、ＣＰＵ１１は、キャンセル要求に含まれるユーザＩＤ及びチケットＮｏ．の組を第１テーブル１４３及び第２テーブル１４４からサーチする（ステップＳ４５４）。そして、サーチされたユーザＩＤ及びチケットＮｏ．の組を第１テーブル１４３及び第２テーブル１４４から削除する（ステップＳ４５５）。これにより、キャンセルしたチケットは使用不能となる。また、ＣＰＵ１１は、当該キャンセル要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグを購入済みを示す２から未予約を示す０に更新する（ステップＳ４５６）。

【０１１０】

フラグの更新が終了すると、ＣＰＵ１１は、キャンセル要求をした携帯電話機３に宛てたメールで、通信装置１３からキャンセル完了通知を送信させる（ステップＳ４５７）。また、キャンセル要求に含まれるユーザＩＤが登録されていないかパスワードが間違っていた場合、或いはキャンセル要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するフラグが購入済みを示していなかった場合には、ＣＰＵ１１は、キャンセル要求をした携帯電話機３に宛てたメールで、通信装置１３からチケットなし通知を送信させる（ステップＳ４５８）。キャンセル完了通知またはチケットなし通知の送信により、サーバ装置１の側における処理は終了となる。

【０１１１】

携帯電話機３では、通信装置３６がステップＳ４５７で送信されたキャンセル完了通知またはステップＳ４５８で送信されたチケットなし通知を受信する（ステップＳ４０３）。ＣＰＵ３１は、受信したキャンセル完了通知またはチケットなし通知を表示装置３５に表示させて、ユーザに示す（ステップＳ４０４）。これで、チケットキャンセル処理が終了する。

【０１１２】

図１１は、チケット再発行処理を示すフローチャートである。チケットを紛失するなどし

て再発行を受けようとするユーザは、自己の携帯電話機３の入力装置３４から、ユーザＩＤとパスワードとを入力する。また、再発行を受けようとするチケットのチケットＮｏ．を入力装置３４から入力する（ステップＳ５０１）。さらにユーザが入力装置から再発行の要求を入力すると、ステップＳ５０１で入力されたユーザＩＤ、パスワード及びチケットＮｏ．と共に再発行要求が通信装置３６からサーバ装置１に送信される（ステップＳ５０２）。その後、ＣＰＵ３１は、サーバ装置１からの情報の受信待ちとなる。

【０１１３】

サーバ装置１では、通信装置１３が携帯電話機３から送られてきた再発行要求を受信する（ステップＳ５５１）。この再発行要求を受信すると、ＣＰＵ１１は、受信した再発行要求に含まれるユーザＩＤがユーザデータベース１４２に登録されているかどうかを判定する。さらに、パスワードが正しいかどうかも判定する（ステップＳ５５２）。

【０１１４】

ユーザＩＤが登録されていて、パスワードも正しい場合には、ＣＰＵ１１は、受信した再発行要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグの状態がチケットの購入済みを示す２になっているかどうかを判定する（ステップＳ５５３）。

【０１１５】

フラグの状態が購入済みを示す２になっていれば、ＣＰＵ１１は、再発行要求に含まれるユーザＩＤ及びチケットＮｏ．の組を第１テーブル１４３及び第２テーブル１４４からサーチする（ステップＳ５５４）。そして、サーチされたユーザＩＤ及びチケットＮｏ．の組を第１テーブル１４３及び第２テーブル１４４から削除する（ステップＳ５５５）。これにより、既に発行されていた再発行前のチケットは使用不能となる。

【０１１６】

既に発行されていたチケットを使用不能とした後、ＣＰＵ１１は、ランダムにパターンを決定して二次元バーコードからなるチケット１００を新たに生成する（ステップＳ５５６）。ＣＰＵ１１は、生成したチケットが既に発行済みのチケット（使用不能とされたものを含まない）のパターンと同じであるかどうかをチェックする発行済みチェック処理を行う（ステップＳ５５７）。発行済みチケットチェック処理は、ステップＳ２５５のものと同じである。

【０１１７】

発行済みチケットチェック処理を終了し、チケット再発行処理に復帰すると、ＣＰＵ１１は、発行済みチケットチェック処理において未発行が返却されたかどうかを判定する（ステップＳ５５８）。発行済みが返却されていた場合には、ステップＳ５５６の処理に戻り、別のパターンを有する二次元バーコードからなるチケット１００を生成する。

【０１１８】

発行済みが返却されていた場合には、ＣＰＵ１１は、共に返却された暗号化値ａ’に対応する第１テーブル１４３の記憶位置と、暗号化値ｂ’に対応する第２テーブル１４４の記憶位置とに、購入要求と共に受信したユーザＩＤとチケットＮｏ．とを組にして登録する（ステップＳ５５９）。ユーザがチケットを購入している状態には変わりないので、ここでのフラグ更新は行われない。

【０１１９】

第１テーブル１４３及び第２テーブルへの登録が終了すると、ＣＰＵ１１は、再発行要求をした携帯電話機３に宛てたメールで、通信装置１３から再発行したチケットの二次元バーコードの画像データを送信させる（ステップＳ５６０）。チケットの画像データを携帯電話機３に送信した後、ＣＰＵ１１は、当該チケットの画像データをサーバ装置１内に残さないように破棄する（ステップＳ５６１）。再発行したチケットを送信し、これを破棄することにより、サーバ装置１の側における処理は終了となる。

【０１２０】

また、再発行要求に含まれるユーザＩＤが登録されていないかパスワードが間違っていた場合、或いは再発行要求に含まれるユーザＩＤ及びチケットＮｏ．に対応するフラグが購

入済みを示していなかった場合には、ＣＰＵ１１は、再発行要求をした携帯電話機３に宛てたメールで、通信装置１３からチケットなし通知を送信させる（ステップＳ５６２）。チケットなし通知の送信により、サーバ装置１の側における処理は終了となる。

【０１２１】

携帯電話機３では、通信装置３６がステップＳ５６０で送信されたチケットまたはステップＳ５７２で送信されたチケットなし通知を受信する（ステップＳ５０３）。ＣＰＵ３１は、受信したチケットまたはチケットなし通知を表示装置３５に表示させて、ユーザに示す（ステップＳ５０４）。これで、チケット再発行処理が終了する。ここで受信したチケットも、ユーザが入力装置３４から所定の操作を行うことで、いつでも表示装置３５に表示させることができる。

【０１２２】

図１２は、チケット認証処理を示すフローチャートである。チケットを購入したユーザが、イベント会場に入場しようとする場合、当該イベントに対応したチケットを自分の携帯電話機３の表示装置３５に表示させる。そして、二次元バーコードからなるチケットが表示された表示装置３５を、入場ゲート装置２のバーコードリーダ２４に押し当てる。

【０１２３】

入場ゲート装置２では、バーコードリーダ２４が携帯電話機３の表示装置３５に表示されたチケットを読み取り、これをＣＰＵ２１に渡す（ステップＳ６０１）。ＣＰＵ２１は、発行時または再発行時にサーバ装置１が行ったのと同じ方法により、読み取ったチケットのパターンに対応した数値Ｘを生成する。チケットの向きは、方向チェックマーク１０１～１０４により分かる（ステップＳ６０２）。さらに、ＣＰＵ２１は、発行時または再発行時にサーバ装置１が行ったのと同様に、チケットを数値化した数値Ｘを除数Ａで除算して剰余ａを求め、また、数値Ｘを除数Ｂで除算して剰余ｂを求める（ステップＳ６０３）。

【０１２４】

ＣＰＵ２１は、さらに、発行時または再発行時にサーバ装置１が行ったのと同様に、求めた剰余ａを所定の暗号鍵を用いて暗号化して暗号化値ａ’を生成し、また、剰余ｂも同様に暗号化して暗号化値ｂ’を生成する（ステップＳ６０４）。ＣＰＵ２１は、生成した暗号化値ａ’、ｂ’を、通信装置２３からサーバ装置１に送信させる（ステップＳ６０５）。

【０１２５】

サーバ装置１では、通信装置１３が入場ゲート装置２から送られてきた暗号化値ａ’、ｂ’を受信する（ステップＳ６５１）。暗号化値ａ’、ｂ’を受信すると、ＣＰＵ１１は、受信した暗号化値ａ’、ｂ’に従ってテーブルチェック処理を行う（ステップＳ６５２）。テーブルチェック処理は、ステップＳ３０４のものと同じである。

【０１２６】

テーブルチェック処理を終了し、チケット認証処理に復帰すると、ＣＰＵ１１は、テーブルチェック処理から返却された情報が一致を示す情報か不一致を示す情報であるかを判定する（ステップＳ６５３）。一致を示す情報であったならば、テーブルチェック処理において第１テーブル１４３及び第２テーブル１４４からユーザＩＤとの組で取り出したチケットＮｏ．が、当該イベントを示すものであるかどうかを判定する（ステップＳ６５４）。

【０１２７】

取り出したチケットＮｏ．が当該イベントを示すものであった場合には、ＣＰＵ１１は、通信装置１３から開放許可通知を入場ゲート装置２に送信させる（ステップＳ６５５）。ＣＰＵ１１は、さらにテーブルチェック処理において第１テーブル１４３及び第２テーブル１４４から取り出したユーザＩＤ及びチケットＮｏ．に対応するユーザデータベース１４２のフラグを購入済みを示す２から使用済みを示す３に更新する（ステップＳ６５６）。

【０１２８】

また、第１テーブル１４３及び第２テーブル１４４から取り出したユーザＩＤ及びチケットＮｏ．の組が一致していなかった場合、或いはチケットＮｏ．が当該イベントを示すものでなかった場合には、ＣＰＵ１１は、通信装置１３からアラーム通知を入場ゲート装置２に送信させる（ステップＳ６５７）。アラーム通知は、第１テーブル１４３及び第２テーブル１４４から取り出したユーザＩＤ及びチケットＮｏ．の組が一致していなかった場合と、チケットＮｏ．が当該イベントを示すものでなかった場合とで内容の異なるものとしてもよい。フラグの更新またはアラーム通知の送信により、サーバ装置１の側における処理は終了となる。

【０１２９】

入場ゲート装置２では、通信装置２３がステップＳ６５５で送信された開放通知またはステップＳ６５７で送信されたアラーム通知を受信する（ステップＳ６０６）。ＣＰＵ２１は、受信したのが開放通知であるかアラーム通知であるかを判定する（ステップＳ６０７）。開放通知であれば、ＣＰＵ２１は、入場ゲート２５を開放状態とさせて、ユーザがイベント会場に入場できるようにする（ステップＳ６０８）。アラーム通知であれば、ＣＰＵ２１は、アラーム装置２６を発報させる（ステップＳ６０９）。入場ゲート２５の開放またはアラームの発報により、チケット認証処理が終了する。

【０１３０】

以上説明したように、この実施の形態にかかるチケット発行システムでは、ユーザが購入したイベントのチケットを携帯電話機３に送信するに当たって、サーバ装置１は、そのチケットに対応した数値Ｘに基づいて暗号化値ａ’、ｂ’を生成し、第１テーブル１４３の暗号化値ａ’に対応する記憶位置と第２テーブル１４４の暗号化値ｂ’に対応する記憶位置とに、ユーザＩＤとチケットＮｏ．の組を登録している。そして、チケットをユーザの携帯電話機３に送信している。

【０１３１】

一方、入場ゲート装置２では、ユーザの携帯電話機３の表示装置３５に表示されたチケットを読み取り、読み取ったチケットを数値化し、暗号化値ａ’、ｂ’を求めて、サーバ装置１に送信している。サーバ装置１では、受信した暗号化値ａ’、ｂ’に従って第１テーブル１４３及び第２テーブル１４４を参照して、チケットが正当なものであるかどうかを認証している。すなわち、二次元バーコードからなるチケットのパターンを照合することなく、第１テーブル１４３と第２テーブル１４４を参照するだけで、チケットの認証を高速に行うことができる。

【０１３２】

チケットのパターンに対応した数値Ｘを除算する除数Ａ、Ｂの最小公倍数は、数値Ｘがとりうる最大値Ｘｍａｘと最小値Ｘｍｉｎの差より大きいという関係がある。この関係を満たす限り、異なるパターンのチケットでは、剰余ａ、ｂの両方が一致することがなく、これらを暗号化した暗号化値ａ’、ｂ’の両方が一致することもない。第１テーブル１４３の暗号化値ａ’に対応する記憶位置と第２テーブル１４４の暗号化値ｂ’に対応する記憶位置とに、同じユーザＩＤ及びチケットＮｏ．の組が登録されるチケットのパターンは、１つだけということとなる。従って、個々のチケットのパターンからユーザ及びチケットＮｏ．を一義的に特定することができる。

【０１３３】

このように第１テーブル１４３及び第２テーブル１４４を参照するだけで、個々のチケットのパターンからユーザ及びチケットＮｏ．を一義的に特定することができるので、発行した各チケットの二次元バーコードのパターンをサーバ装置１に残しておく必要がない。二次元バーコードのパターンは、情報量が大きくなるものなので、これを残さないでよいことから、サーバ装置１の記憶容量が小さくても済むことになる。

【０１３４】

また、チケットのパターンは、サーバ装置１に残さないでよいことから、サーバ装置１をハッキングしても盗み出されることがないので、セキュリティが高いものとなる。ハッキングに備えて暗号化して保存するのと異なり、チケットの発行時においてチケットのパタ

ーンを暗号化したり、チケットの認証時においてチケットのパターンを復号化するという処理は必要ない。このため、高度のセキュリティを達成しつつ、サーバ装置１の処理量を小さくすることができる。

【０１３５】

もっとも、剰余ａ、ｂと、除数Ａ、Ｂと、チケットのパターンから数値Ｘを生成する方法が分かってしまえば、チケットのパターンを復元できてしまう。ところが、第１テーブル１４３及び第２テーブル１４４にユーザＩＤ及びチケットＮｏ．の組を登録する記憶位置は、剰余ａ、ｂに対応する記憶位置ではなく、暗号化値ａ’、ｂ’に対応した記憶位置としている。

【０１３６】

ユーザＩＤ及びチケットＮｏ．の組の記憶位置から暗号化値ａ’、ｂ’の値は分かってしまうが、暗号化値ａ’、ｂ’を復号化する処理は一切行う必要がないので、これを復号化する復号鍵は、サーバ装置１にも入場ゲート装置２にも置いていない。このため、サーバ装置１及び入場ゲート装置２がハッキングされても、剰余ａ、ｂの値を知ることができないので、ここから不正に読み出された情報のみに基づいてチケットのパターンを復元することはできない。

【０１３７】

仮にチケットのパターンを復元しようとするのであれば、オブジェクトコードで記述されたプログラムを解析して除数Ａ、Ｂを抜き出し、チケットのパターンから数値Ｘを生成する方法を解読し、さらに第１テーブル１４３及び第２テーブル１４４に対応したアドレスと暗号化値ａ’、ｂ’との関係を解読しなければならない。その上で、暗号化値ａ’、ｂ’を剰余ａ、ｂに復号化する復号鍵を見つけ出さなければならない。このため、剰余ａ、ｂの暗号化強度がそれほど高くなくても、全体としては、最強と呼ばれるような暗号アルゴリズムに比べても遜色がない、或いはそれ以上のセキュリティを達成することができるようになる。

【０１３８】

また、第１テーブル１４３及び第２テーブル１４４には、ユーザＩＤだけでなく、チケットＮｏ．も組み合わせて登録している。第１テーブル１４３及び第２テーブル１４４から取り出したユーザＩＤとチケットＮｏ．の両方が一致していなければ、イベント会場への入場はできない。このため、１人のユーザが異なるイベントについて複数のチケットを購入して使えるようにしても、各イベントに対してチケットを購入したユーザだけが、当該イベントの会場に入場できるようにすることができる。

【０１３９】

さらに、１人のユーザが複数のチケットを購入して使えるようにすることで、チケットとして発行される二次元バーコードの数がユーザ数よりも大幅に増えることとなる。しかし、ユーザの携帯電話機３に送信した後は二次元バーコードからなるチケットを保存せず、また、二次元バーコード同士を照合することも一切行っていない。このため、チケットの数の増加による処理量や記憶容量の増加は、チケットの数の増加に比べると無視できる程度に僅かなものとすることができる。

【０１４０】

この実施の形態にかかるチケット発行システムでは、上記したように必要となる処理量や記憶容量が大きく増えることはないので、複雑なパターンの二次元バーコードをチケットに適用することができる。複雑なパターンの二次元バーコードを使用することで、適当に生成したパターンが各イベントについて発行したチケットのパターンと一致する確率は、数万～数百万分の１以下という極めて小さな値とすることもできる。

【０１４１】

また、発行済みのチケットに適用された二次元バーコードのパターンは、サーバ装置１にも入場ゲート装置２にも残っておらず、チケットを購入したユーザの携帯電話機３においてのみ管理されるだけである。このため、偽造のチケットによりイベント会場に不正な入場があった場合、その責任はユーザ側にある場合がほとんどである。従って、システムの

提供者がイベントの開催者から、不正な入場に対する責任を問われる場合がほとんどなくて済むようになる。

【０１４２】

ところで、上記のチケット発行システムにおける処理は、チケット予約処理、チケット購入処理、チケットキャンセル処理、チケット再発行処理、及びチケット認証処理の５つに大きく分けられるが、このうちで短時間のうちに処理が集中すると考えられるのは、チケット予約処理とチケット認証処理の２つだけである。チケット購入処理、チケットキャンセル処理、チケット再発行処理は、チケットの予約を行った後、イベントの開始までの任意の時に行われるものだからである。

【０１４３】

チケットに適用される二次元バーコードのパターンの生成や、数値化、剰余の算出、暗号化値の生成といった比較的処理量が大きい（もっとも、バーコードの照合に比べれば小さいが）処理は、処理の集中する時間においてサーバ装置１が実行する必要がない。チケット認証処理においては、処理が集中する時間に入場ゲート装置２が読み取ったチケットの数値化、剰余の算出、暗号化値の生成といった比較的処理量が大きい処理を行わなければならないが、入場ゲート装置２は実際には複数あって、それぞれに処理を分散できる。

【０１４４】

このため、チケット予約処理及びチケット認証処理に対応するため、必要以上に処理能力が高いサーバ装置１を用意しておく必要がない。また、比較的処理量が大きい処理は分散して行われるため、サーバ装置１を無駄なく稼働させることができるようになる。

【０１４５】

本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について説明する。

【０１４６】

上記の実施の形態では、サーバ装置１は、ユーザＩＤとパスワードとを用いて、ユーザデータベース１４２に登録されたユーザを認証し、特定するものとしていた。これに対して、サーバ装置１が自動音声応答によりチケットの購入予約や販売等の処理を行うものとする場合、携帯電話機３からの着呼時に通知される発信者番号を用いて、ユーザデータベース１４２に登録されたユーザを認証し、特定するものとしてもよい。

【０１４７】

上記の実施の形態では、チケットに対応した数値を、そのまま除数Ａ、Ｂで除算して、剰余ａ、ｂを求めるものとしていた。これに対して、チケットに対応した数値から該数値がとり得る最小値を減算した値、またはチケットに対応した数値がとり得る値の最大値からチケットに対応する数値を減算した値を、数値Ａ、Ｂで除算して、剰余ａ、ｂを求めるものとしてもよい。この場合、チケットに対応した数値がとり得る値の範囲によっては、被除数がかなり小さくなって、除算の処理が高速化される。

【０１４８】

上記の実施の形態では、チケットの認証を行うために、第１テーブル１４３と第２テーブル１４４の２つのテーブルを用いていた。これに対して、３つ以上のテーブルを用いてチケットの認証を行うものとしてもよい。チケットに対応した数値は、それぞれのテーブル毎に異なる除数で除算して剰余を求めるものとすることができる。３つ以上の除数の最小公倍数が、チケットに対応した数値の最大値と最小値との差よりも大きくなればよい。さらにそれぞれの剰余を暗号化した暗号化値に従って、各テーブルを参照するものとすればよい。３つ以上のテーブルを用いた場合には、全てのテーブルでユーザＩＤとチケットＮｏ．の組が一致するかどうかを調べるものとすればよい。

【０１４９】

上記の実施の形態では、チケットに対応した数値を除数Ａ、Ｂで除算した剰余を求め、さらにこれを暗号化した暗号化値ａ’、ｂ’を生成していた。この暗号化値ａ’、ｂ’の組み合わせは、チケットのパターン毎に異なるものとなっていた。しかしながら、チケットに対応した数値から求められる複数の数値の組がチケットのパターン毎に異なるものとな

るのであれば、上記とは別の演算式を適用することができる。さらに、チケットを複数の領域に分割し、各領域をそのまま数値化した複数の数値の組は、チケットのパターン毎に異なるものとなるので、上記したような演算で求められる数値の組に代えて適用することもできる。

【０１５０】

上記の実施の形態では、チケットに対応した数値を除算した後の剰余だけを暗号化するものとしていた。これに対して、サーバ装置１及び入場ゲート装置２では、チケットのパターンを数値化した後に暗号化し、暗号化した数値を除算して剰余を求めるものとしてもよい。この剰余をさらに暗号化するものとしてもよい。ここで、チケットに対応した数値を暗号化する暗号鍵にも、復号鍵が異なる非対称暗号系の暗号鍵を適用することができる。ここでも、暗号化した数値の復号化を一切行う必要がないからである。この場合には、サーバ装置１から情報が盗み出されても、盗み出した情報からチケットを復元することはさらに困難となるので、よりセキュリティの高いシステムを構成することができる。

【０１５１】

上記の実施の形態では、サーバ装置１は、チケットを販売または再発行する際に、二次元バーコードによるパターンを生成してから、これを数値化するものとしていた。これに対して、ランダムに生成した数値から暗号化値ａ’、ｂ’までを求め、第１テーブル１４３及び第２テーブル１４４を参照した結果として発行済みでないことが分かってから、数値に対応したパターンを生成して二次元バーコードのチケットとして携帯電話機３に宛てて送信するものとしてもよい。この場合、実際には使用できないチケットはパターンまでを生成する必要がなくなるので、余分な処理が行わないで済むようになる。

【０１５２】

上記の実施の形態では、チケットとして用いられる二次元バーコードのパターンは、サーバ装置１から携帯電話機３に送られると、すぐに表示装置３５に表示できるものとしていた。しかし、この場合には、表示装置３５に表示されたパターンを見た者が同じ画像を生成して、チケットを偽造することができるようになってしまう。そこで、所定の暗証番号を入力しなければ、送信した二次元バーコードのパターンを表示装置３５に表示できないようにしてもよい。入場ゲート装置２の直前で暗証番号を提示すれば、正規に販売したチケットと同じパターンを予め生成しておくことが実施的に不可能となり、不正なチケットによるイベント会場への不正入場を防ぐことができるようになる。

【０１５３】

上記の実施の形態では、ユーザが購入したチケットまたは再発行を受けたチケットは、携帯電話機３にメールで送信されるものとしていた。しかしながら、ユーザがメールの転送設定を行っていれば、本当はチケットを購入していない者にもチケットを含むメールが送られてしまうこととなる。これに対して、携帯電話会社の公式サイトとしてチケットの販売等を行えば、サーバ装置１が携帯電話機３から購入要求や再発行要求を受信したときに、ユーザの携帯電話機３の個体番号が通知されてきている。

【０１５４】

そこで、サーバ装置１は、通知された個体番号を暗号鍵として用いてチケットを暗号化して送信し、携帯電話機３において個体番号を復号鍵として用いて復号するようにしてもよい。これにより、本当はチケットを購入していない者にチケットを含むメールが転送されても、その二次元バーコードのパターンを正しく復号して表示できなくなる。これにより、サーバ装置１から携帯電話機３への送信途中で盗み出されたチケットや、不正に転送されたチケットによるイベント会場への不正入場を防ぐことができるようになる。

【０１５５】

上記の実施の形態では、チケットは、二階調の二次元バーコードによって構成され、携帯電話機３の表示装置３５に表示されるものとしていた。これに対して、多階調のパターンを有するバーコードや、三次元のパターンを有するバーコードをチケットに適用することもできる。この三次元バーコードは、例えばポリゴンで形成された立方体の各面に二次元のバーコードを表示させたものであり、Ｊａｖａ（登録商標）等のアプリケーションによ

ってポリゴンが回転される。入場ゲート装置２のＣＰＵ２１は、ポリゴンの回転によって立方体の各面に表示されたコードを全て認識することができる。三次元バーコードは、二次元バーコードより情報量を大きくすることができるが、三次元バーコードのように情報量が大きい識別情報では、必要な記憶容量を小さくできるという効果が顕著に現れる。

【０１５６】

入場ゲート装置２と携帯電話機３とをブルートゥース技術の適用などにより直接通信可能に構成した場合には、チケットして視認不可能な情報であっても、上記した二次元バーコードの代わりに適用することができる。どのような形態の識別情報であっても、それを数値化した後に上記の実施の形態と同様に暗号化値ａ’、ｂ’までを求め、この暗号化値ａ’、ｂ’を用いて、第１テーブル１４３及び第２テーブル１４４を参照するという構成を採用することができる。

【０１５７】

上記の実施の形態では、イベントのチケットを二次元バーコードによって構成した場合に、その認証のための技術として本発明を適用した場合について説明した。しかしながら、本発明の適用範囲はイベントのチケットに限るものではなく、１人のユーザが複数の識別情報を使い分けて認証を受ける場合全般に適用することができる。

【０１５８】

上記の実施の形態では、サーバ装置１、入場ゲート装置２、及び携帯電話機３の処理プログラムは、それぞれ主記憶装置１２、記憶装置２２、或いはＲＯＭ３２に予め記憶されているものとして説明した。これに対して、これらの処理プログラムの全部または一部のみをＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に格納して、ハードウェアとは別に配布するものとしてもよい。また、これらの処理プログラムの全部または一部をインターネット上のＷｅｂサーバ装置が有する固定ディスク装置に格納しておき、サーバ装置１、入場ゲート装置２、或いは携帯電話機３からの要求に従って、インターネットなどのネットワークを通じて配信するものとしてもよい。

【０１５９】

【発明の効果】

以上説明したように、本発明によれば、識別情報の発行及び認証において、認証処理の高速化とセキュリティの向上とを同時に達成することができる。

【０１６０】

また、識別情報の発行及び認証において、例えば１人のユーザが複数の識別情報を使い分けることなどにより、発行される識別情報の数が増えても、処理量をあまり増大させることがない。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかるチケット発行システムを示すブロック図である。

【図２】図１のサーバ装置の構成を示すブロック図である。

【図３】二次元バーコードにより構成されるチケットの例を示す図である。

【図４】図２のユーザデータベースと、第１、第２のテーブルを示す図である。

【図５】図１の携帯電話機の構成を示すブロック図である。

【図６】図１の入場ゲート装置の構成を示すブロック図である。

【図７】チケット予約処理を示すフローチャートである。

【図８】チケット購入処理を示すフローチャートである。

【図９】図８の発行済みチケットチェック処理を詳細に示すフローチャートである。

【図１０】チケットキャンセル処理を示すフローチャートである。

【図１１】チケット再発行処理を示すフローチャートである。

【図１２】チケット認証処理を示すフローチャートである。

【符号の説明】

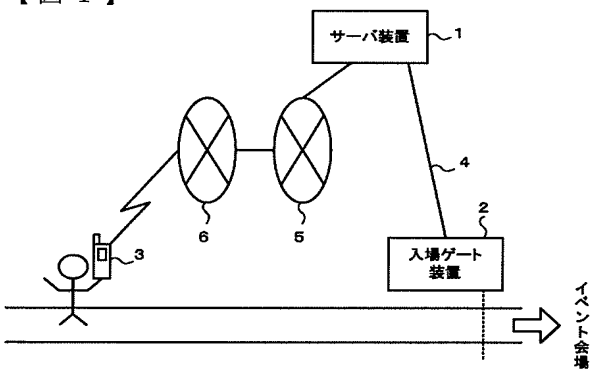
１　サーバ装置

２　入場ゲート装置

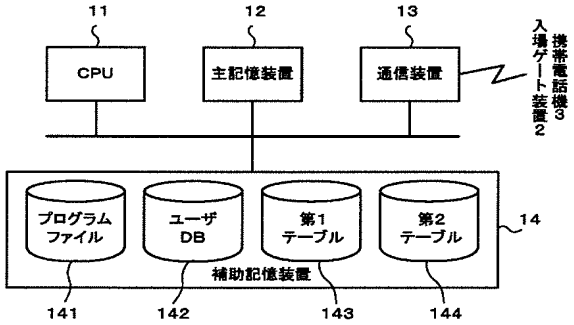
３　携帯電話機

４　専用線
５　インターネット
６　携帯電話網
１１　ＣＰＵ
１２　主記憶装置
１３　通信装置
１４　補助記憶装置
２１　ＣＰＵ
２２　記憶装置
２３　通信装置
２４　バーコードリーダ
２５　入場ゲート
３１　ＣＰＵ
３２　ＲＯＭ
３３　ＲＡＭ
３４　入力装置
３５　表示装置
３６　通信装置
１００　チケット（二次元バーコード）
１０１～１０４　方向チェックマーク
１０５　チケット表示部
１４１　プログラムファイル
１４２　ユーザデータベース
１４３　第１テーブル
１４４　第２テーブル

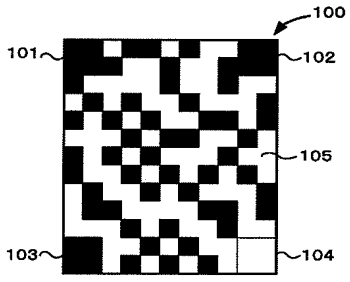
【図１】



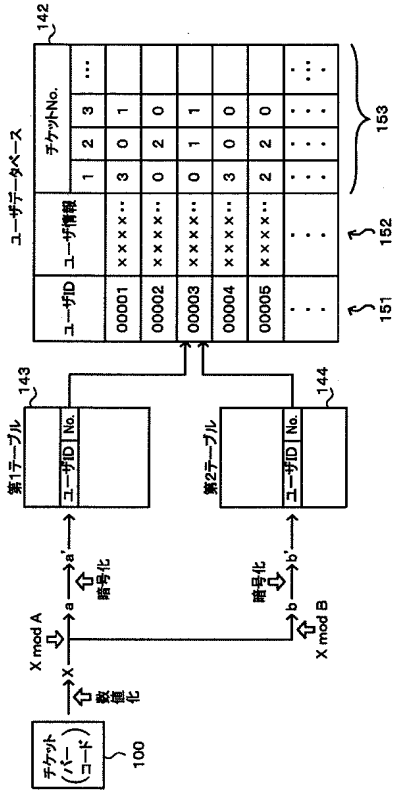
【図２】



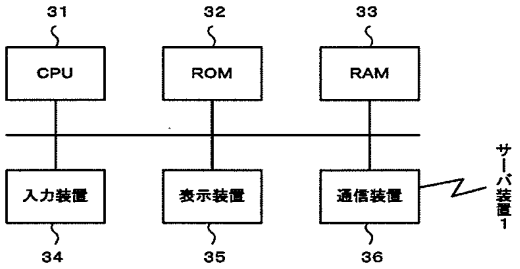
【図３】



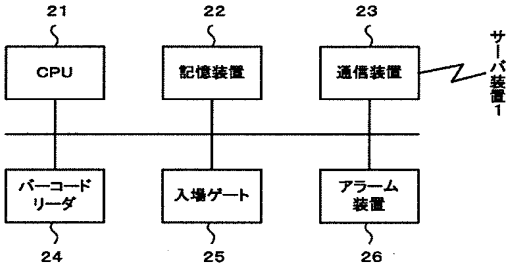
【図４】


142
ユーザデータベース
ユーザID
ユーザ情報
チケットNo.
1
2
3
00001
00002
00003
00004
00005
151
152
153
143
第1テーブル
144
第2テーブル
No.
暗号化
X mod A
X mod B
チケット（バーコード）
100

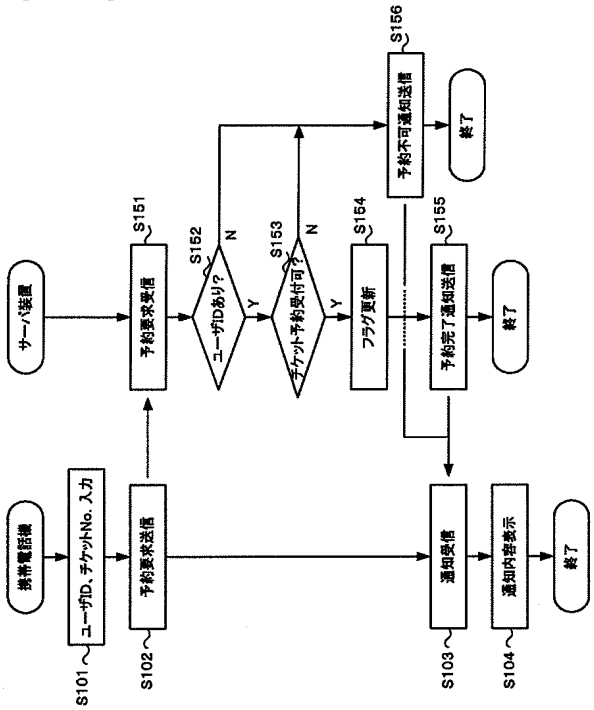
【図５】


31
32
33
CPU
ROM
RAM
入力装置
表示装置
通信装置
サーバ装置1
34
35
36

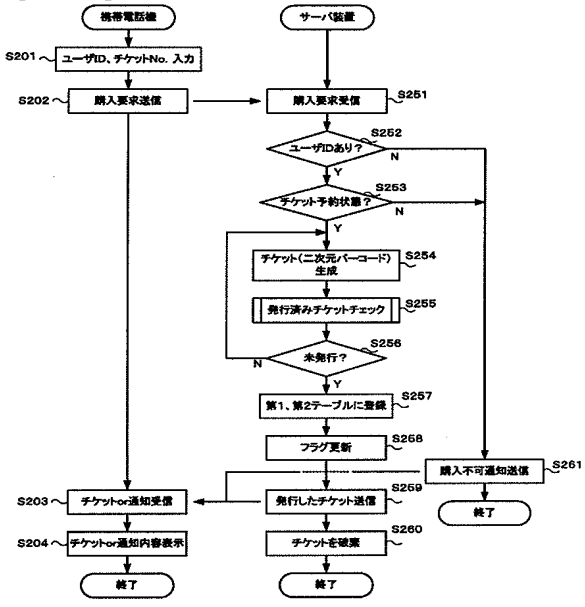
【図６】


21
22
23
CPU
記憶装置
通信装置
サーバ装置1
バーコードリーダ
入場ゲート
アラーム装置
24
25
26

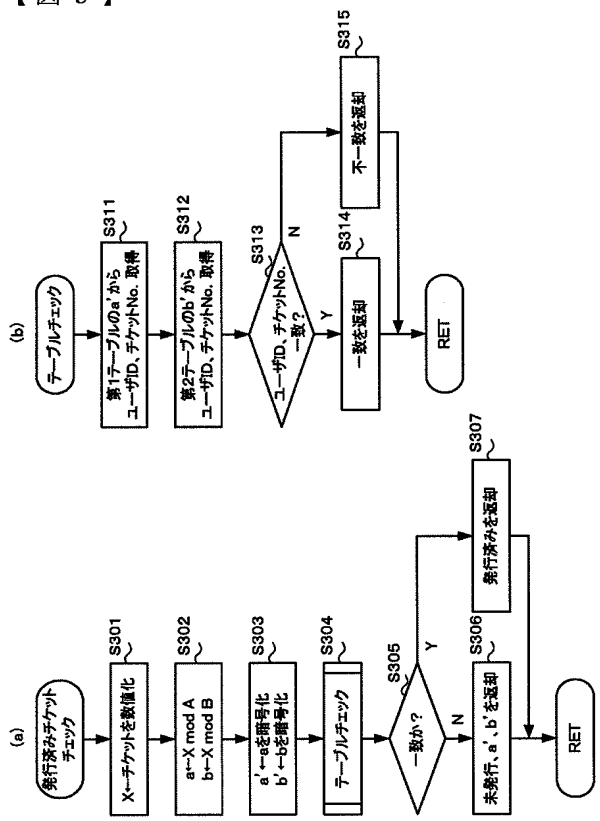
【図７】


サーバ装置
予約要求受信
S151
ユーザIDあり？
S152
N
Y
チケット予約受付可？
S153
N
Y
フラグ更新
S154
予約完了通知送信
S155
予約不可通知送信
S156
終了
終了
携帯電話機
ユーザID、チケットNo. 入力
予約要求送信
通知受信
通知内容表示
終了
S101
S102
S103
S104

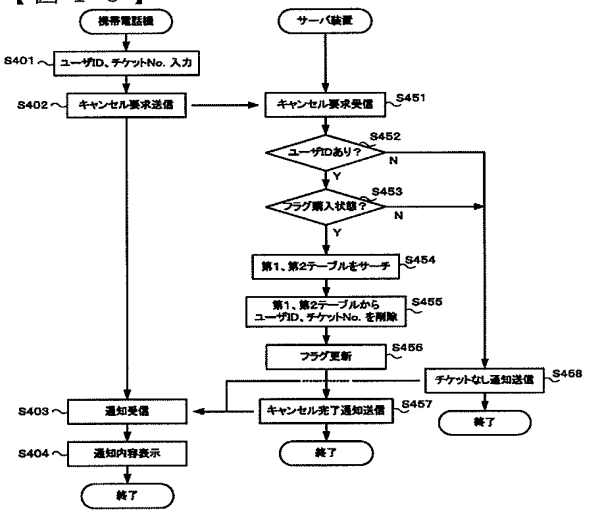
【図８】


携帯電話機
サーバ装置
S201
ユーザID、チケットNo. 入力
S202
購入要求送信
購入要求受信
S251
ユーザIDあり？
S252
N
Y
チケット予約状態？
S253
N
Y
チケット（二次元バーコード）生成
S254
発行済みチケットチェック
S255
未発行？
S256
N
Y
第1、第2テーブルに登録
S257
フラグ更新
S258
購入不可通知送信
S261
終了
S203
チケットor通知受信
S204
チケットor通知内容表示
終了
発行したチケット送信
S259
チケットを破棄
S260
終了

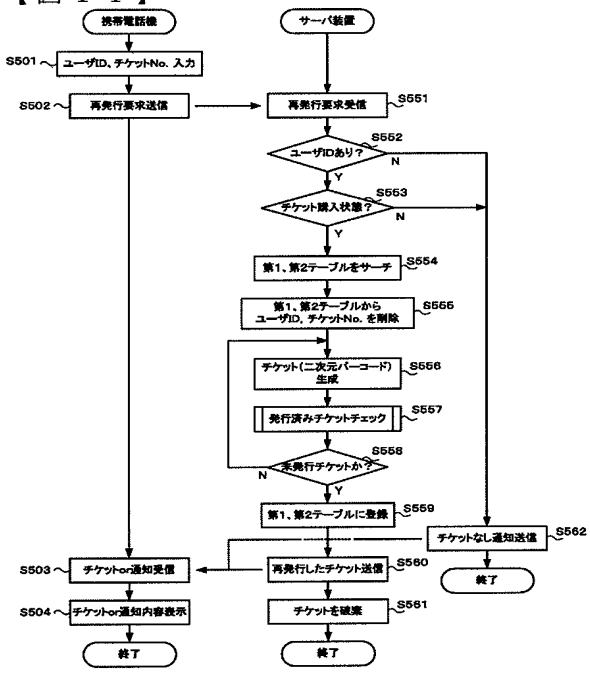
【図９】



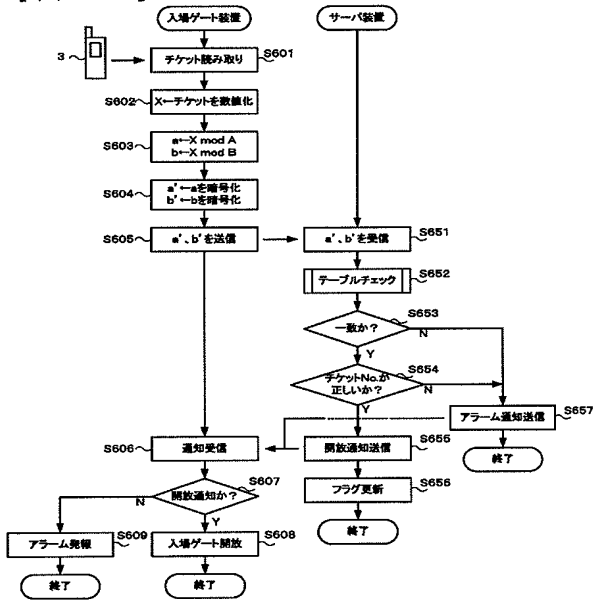
【図１０】



【図１１】



【図１２】



フロントページの続き

(51) Int.Cl.[7]		FI			テーマコード（参考）
Ｇ０６Ｋ	17/00	Ｇ０６Ｋ	7/10	Ｚ	５Ｊ１０４
Ｇ０６Ｋ	19/07	Ｇ０６Ｋ	17/00	Ｔ	
Ｇ０９Ｃ	1/00	Ｇ０９Ｃ	1/00	６５０Ｚ	
Ｈ０４Ｌ	9/32	Ｈ０４Ｌ	9/00	６７５Ｂ	
		Ｇ０６Ｋ	19/00	ＺＥＣＪ	

Ｆターム(参考) 5B082 EA11
5B085 AA08 AE09 AE15 AE23 AE29 BE04 BG02 CA02 CA04 CA07
5J104 AA12 KA05 NA02 NA18